UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/711,323	11/09/2000	Alfonso de Jesus Valdes	10454-014002	6879

52197 7590 12/29/2005

MOSER, PATTERSON & SHERIDAN, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/711,323	VALDES ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 1 December 2005.

2. Claims 1-9 are pending in the application.

3. Claims 1-9 have been rejected.

Response to Arguments

4. On page 5, the applicant argues that claims 7 and 9 of the present application are patentably distinct from claims 1 and 3 of the 09/944,788 application.

The examiner respectfully disagrees. The claims of the current application are broader than the claims of the 09/944,788 application.

5. Applicant's arguments with respect to claims 1-9 have been considered but are moot in view of the new ground(s) of rejection.

Double Patenting

6. Claims 7 and 9 of this application conflict with claims 1 and 3 of Application No. 09/944,788. 37 CFR 1.78(b) provides that when two or more applications filed by the same applicant contain conflicting claims, elimination of such claims from all but one application may be required in the absence of good and sufficient reason for their retention during pendency in more than one application. Applicant is required to either cancel the conflicting claims from all but one application or maintain a clear line of demarcation between the applications. See MPEP § 822.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 2, 4 and 5 are rejected under 35 U.S.C. 102(e) as being anticipated by Baker U.S. Patent No. 6,775,657 B1.

As to claim 1, Baker discloses a method for correlating a first sensor to a second sensor in an intrusion detection system, the first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor information about the second sensor's belief state, the belief state indicating a state of at least one system resource or service [column 7 line 27 to column 8 line 47]; and

(b) adjusting a prior belief state of the first sensor, the belief state indicating a state of at least one system resource or service, the adjustment is based at least in part on the second sensor's belief state [column 7 line 27 to column 8 line 47].

As to claim 2, Baker discloses that the first and second sensors are different types of sensors [column 7 line 27 to column 8 line 47].

As to claim 4, Baker discloses a method of reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion

detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding an apparent normal, degraded or compromised state of a monitored resource [column 7 line 27 to column 8 line 47]; and

(b) adjusting a prior belief state of the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm [column 7 line 27 to column 8 line 47].

As to claim 5, Baker discloses a method of enhancing the sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding the existence or validity of services supported on monitored computer system resources [column 7 line 27 to column 8 line 47]; and

(b) adjusting a prior belief state of the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious [column 7 line 27 to column 8 line 47].

8. Claims 6-9 are rejected under 35 U.S.C. 102(e) as being anticipated by Bristol U.S. Patent No. 6,690,274 B1.

As to claim 6, Bristol discloses a method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) identifying a set of potentially similar features shared by a new alert and one or more existing alert classes [column 17 line 24 to column 18 line 63];

(b) comparing the new alert to one or more existing alert classes [column 17 line 24 to column 18 line 63];

(c) adjusting the comparison by an expectation that certain feature values will or will not match [column 17 line 24 to column 18 line 63];

(d1) associating the new alert with the existing alert class that the new alert most closely matches [column 17 line 24 to column 18 line 63].

As to claim 7, Bristol discloses a method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) receiving a new alert [column 24, lines 23-29];

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes, as discussed above;

(c) updating a similarity expectation for one or more feature values [column 24 line 58 to column 25 line 36];

(d) comparing the new alert with one or more alert classes, as discussed above;

(e1) associating the new alert with the existing alert class that the new alert most closely matches, as discussed above.

As to claim 8, Bristol discloses passing each existing alert class through a transition model to generate a new prior belief state for each alert class [column 24 line 58 to column 25 line 36].

As to claim 9, Bristol discloses a method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) generating a group of feature records for a new alert, each feature record includes a list of observed values for its corresponding feature [column 24, lines 23-29];

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that: are associated with previous alerts, as discussed above;

(c) comparing the new alert to one or more alert classes, as discussed above;

(d) adjusting the comparison by an expectation that certain feature values will or will not match, as discussed above; and

(e1) associating the new alert with the existing alert class that the new alert most closely matches, as discussed above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baker U.S. Patent No. 6,775,657 B1 as applied to claim 1 above, and further in view of Timm U.S. Patent No. 5,440,498.

As to claim 3, Baker does not teach that the first sensor is a probabilistic sensor.

Timm teaches a probabilistic sensor in intrusion detection systems [column 5, lines 7-46].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baker so that the first sensor would have been a probabilistic sensor.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baker by the teaching of Timm because it provides that ability to compare the effectiveness of any security element or group of elements of the security system with another element or group of elements. Not only does this method reveal the less effective security elements of a system, but also it can be employed to evaluate whether proposed additions to a security system would enhance protection of the facility and, if so, by how much [column 2, lines 16-29].

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy AM
December 23, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100